

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

## CLAIMS

What is claimed is:

- 1 1. In a video source device, a method comprising:  
2 generating a session key for a transmission session within which a multi-  
3 frame video content is to be transmitted to a video sink device; and  
4 generating a successive number of frame keys, using at least the session  
5 key, to facilitate ciphering of corresponding frames of the multi-frame video content  
6 for transmission to the video sink device.
- 1 2. The method of claim 1, wherein said generating of successive frame keys  
2 comprises generating at each vertical blanking interval of said multi-frame video  
3 content, a frame key for ciphering a frame of said multi-frame video content.
- 1 3. The method of claim 2, wherein said method further comprises generating a  
2 pseudo random bit sequence for each frame, using at least the corresponding frame  
3 key, for ciphering the particular frame of said multi-frame video content.
- 1 4. The method of claim 3, wherein each of said generating of a pseudo random  
2 bit sequence using a corresponding frame key comprises successive modifications  
3 of the corresponding frame key.
- 1 5. The method of claim 4, wherein said successive modifications of the  
2 corresponding frame key are performed at horizontal blanking intervals of the frame.

1 6. The method of claim 3, wherein said method further comprises generating an  
2 initial pseudo random bit sequence using at least the session key, and deriving an  
3 initial pseudo random number from the initial pseudo random bit sequence to be  
4 used with a first frame key to generate a first pseudo random bit sequence to cipher  
5 a first frame.

1 7. The method of claim 3, wherein each of said generating of a pseudo random  
2 bit sequence comprises generating sufficient number of pseudo random bits for  
3 ciphering a pixel on a bit-wise basis each clock.

1 8. In a video source device, a method comprising:  
2 generating a frame key for each frame of a multi-frame video content; and  
3 generating a pseudo random bit sequence for each of the corresponding  
4 frames, using at least the corresponding frame key, for ciphering the video content.

1 9. The method of claim 8, wherein said generating of a frame key for each  
2 frame comprises generating one frame key at each vertical blanking interval of said  
3 multi-frame video content.

1 10. The method of claim 8, wherein said method further comprises generating an  
2 initial pseudo random bit sequence, deriving an initial pseudo random number from  
3 the initial pseudo random bit sequence to be used with the first frame key to  
4 generate a first pseudo random bit sequence to cipher a first frame.

1 11. The method of claim 8, wherein each of said generating of a pseudo random  
2 bit sequence using a corresponding frame key comprises successive modifications  
3 of the corresponding frame key at horizontal blanking intervals of the frame.

1 12. In a video source device, a method comprising:  
2 generating a frame key at each vertical blanking interval of a multi-frame  
3 video content; and  
4 generating a pseudo random bit sequence for each frame of said multi-frame  
5 video content, using at least the corresponding frame key for ciphering the particular  
6 frame, with generation of each pseudo random bit sequence including successive  
7 modifications of the corresponding frame key at horizontal blanking intervals of the  
8 corresponding frame.

1 13. An apparatus comprising:  
2 a block cipher to generate a session key for a transmission session within  
3 which a multi-frame video content is to be transmitted to the video sink device, and  
4 to generate a successive number of frame keys, using the session key, for  
5 corresponding frames of said multi-frame video content; and  
6 a stream cipher coupled to the block cipher to generate a pseudo random bit  
7 sequence for each frame, using at least the corresponding frame key, for ciphering  
8 the particular frame of said multi-frame video content for transmission.

1 14. The apparatus of claim 13, wherein the stream cipher comprises a register to  
2 successively store a frame key associated with each frame.

1 15. The apparatus of claim 14, wherein the stream cipher further comprises a  
2 **stream key section** coupled to the register to be programmed with **the same** frame  
3 key, to generate first data bits to successively modify the register stored **frame key**  
4 to facilitate generation of the pseudo random bit sequence for the frame.

1 16. The apparatus of claim 14, wherein the stream cipher further comprises a  
2 first function block coupled to the register to successively transform a stored frame  
3 key and a second function block coupled to the register to generate a pseudo  
4 random bit sequence for the corresponding frame using a selected subset of each of  
5 the transformed states of the frame key.

1 17. The apparatus of claim 13, wherein the block cipher comprises a first and a  
2 second register to store a first and a second value, and a function block coupled to  
3 the first and second registers to transform the stored first and second values, with a  
4 selected one of the transformed first and second values being the session key or a  
5 frame key.

1 18. The apparatus of claim 17, wherein the block cipher is an integral part of said  
2 stream cipher.

1 19. In a video sink device, a method comprising:  
2 generating a session key for a reception session within which a multi-frame  
3 video content is to be received from a video source device; and  
4 generating a successive number of frame keys, using at least the session  
5 key, to facilitate deciphering of corresponding frames of the multi-frame video  
6 content received from the video source device.

1 20. The method of claim 19, wherein said generating of successive frame keys  
2 comprises generating at each vertical blanking interval of said multi-frame video  
3 content, a frame key for deciphering a frame of said multi-frame video content.

1 21. The method of claim 20, wherein said method further comprises generating a  
2 pseudo random bit sequence for each frame, using at least the corresponding frame  
3 key, for deciphering the particular frame of said multi-frame video content.

1 22. The method of claim 21, wherein each of said generating of a pseudo  
2 random bit sequence using a corresponding frame key comprises successive  
3 modifications of the frame key.

1 23. The method of claim 22, wherein said successive modifications are  
2 performed at horizontal blanking intervals of the frame.

1 24. The method of claim 21, wherein said method further comprises generating  
2 an initial pseudo random bit sequence using at least the session key, and deriving  
3 an initial pseudo random number from the initial pseudo random bit sequence to be  
4 used with the first frame key to generate a first pseudo random bit sequence to  
5 cipher a first frame.

1 25. The method of claim 21, wherein each of said generating of a pseudo  
2 random bit sequence comprises generating sufficient number of pseudo random bits  
3 for deciphering a pixel on a bit-wise basis each clock.

1 26. In a video sink device, a method comprising:  
2 generating a frame key for each frame of a multi-frame video content  
3 received from a video source device; and  
4 generating a pseudo random bit sequence for each of the corresponding  
5 frames, using at least the corresponding frame key, for ciphering the video content.

1 27. The method of claim 26, wherein said generating of a frame key for each  
2 frame comprises generating one frame key at each vertical blanking interval of said  
3 multi-frame video content.

1 28. The method of claim 26, wherein said method further comprises generating  
2 an initial pseudo random bit sequence, deriving an initial pseudo random number  
3 from the initial pseudo random bit sequence to be used with the first frame key to  
4 generate a first pseudo random bit sequence to cipher a first frame.

1 29. The method of claim 28, wherein each of said generating of a pseudo  
2 random bit sequence comprises successively modifying the frame key at horizontal  
3 blanking intervals of the frame.

1 30. In a video sink device, a method comprising:  
2 generating a frame key at each vertical blanking interval of a multi-frame  
3 video content to be received from a video source device; and  
4 generating a pseudo random bit sequence for each frame of said multi-frame  
5 video content, using at least the corresponding frame key and a pseudo random  
6 number, for ciphering the particular frame, with generation of each pseudo random  
7 bit sequence including successive modifications of the corresponding pseudo

8 random using using the corresponding frame key at horizontal blanking intervals of  
9 the corresponding frame.

1 31. An apparatus comprising:

2 a block cipher to generate a session key for a transmission session within  
3 which a multi-frame video content is to be received from a video sink device, and to  
4 generate a successive number of frame keys; using the session key, for  
5 corresponding frames of said multi-frame video content; and

6 a stream cipher coupled to the block cipher to generate a pseudo random bit  
7 sequence for each frame, using at least the corresponding frame key, for  
8 deciphering the particular frame of said multi-frame video content.

1 32. The apparatus of claim 31, wherein the stream cipher comprises a register to  
2 successively store a frame key associated with each frame.

1 33. The apparatus of claim 32, wherein the stream cipher further comprises a  
2 stream key section coupled to the register to be programmed with a frame key  
3 associated with the same frame, to generate first data bits to successively modify  
4 the register stored frame key to facilitate generation of the pseudo random bit  
5 sequence for the frame.

1 34. The apparatus of claim 32, wherein the stream cipher further comprises a  
2 first function block coupled to the register to successively transform a stored frame  
3 key, and a second function block coupled to the register to generate the pseudo  
4 random bit sequence for the corresponding frame using a selected subset of each of  
5 the transformed states of the frame key.



1 35. The apparatus of claim 31, wherein the block cipher comprises a first and a  
2 second register to store a first and a second value, and a function block coupled to  
3 the first and second registers to successively transform the stored first and second  
4 values, with a selected one of the transformed first and second values being the  
5 session key or a frame key.

1 36. The apparatus of claim 35, wherein the block cipher is an integral part of said  
2 stream cipher.